

Lower Bounds for Maximum Gap in (Inverse) Cyclotomic Polynomials

Mary Ambrosino, Hoon Hong, Eunjeong Lee

February 27, 2017

Abstract

The maximum gap $g(f)$ of a polynomial f is the maximum of the differences (gaps) between two consecutive exponents that appear in f . Let Φ_n and Ψ_n denote the n -th cyclotomic and n -th inverse cyclotomic polynomial, respectively. In this paper, we give several lower bounds for $g(\Phi_n)$ and $g(\Psi_n)$, where n is the product of odd primes. We observe that they are very often exact. We also give an exact expression for $g(\Psi_n)$ under a certain condition. Finally we conjecture an exact expression for $g(\Phi_n)$ under a certain condition.

1 Introduction

The n -th cyclotomic and n -th inverse cyclotomic polynomials are defined as follows

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ (k,n)=1}} \left(x - e^{2\pi i \frac{k}{n}} \right) \quad \Psi_n(x) = \prod_{\substack{1 \leq k \leq n \\ (k,n) \neq 1}} \left(x - e^{2\pi i \frac{k}{n}} \right)$$

For example, we have

$$\begin{aligned} \Phi_{15}(x) &= 1 - x + x^3 - x^4 + x^5 - x^7 + x^8 \\ \Psi_{15}(x) &= -1 - x - x^2 + x^5 + x^6 + x^7 \end{aligned}$$

There have been extensive studies on the coefficients of cyclotomic polynomials [21, 4, 3, 11, 19, 15, 14, 25, 5, 16, 12, 6, 24, 10, 13, 7, 8], and more recently, on inverse cyclotomic polynomials [22, 5, 8].

In [17], a study was initiated on their exponents, in particular on the maximum gap g , that is, the largest difference between consecutive exponents: for example, $g(\Phi_{15}) = 2$ since 2 is the maximum among $1-0, 3-1, 4-3, 5-4, 7-5, 8-7$. The original motivation came from elliptic curve cryptography; the computing time of the Ate_i pairing over elliptic curves depends on the maximum gap of the inverse cyclotomic polynomials whose degree are decided from the parameter of the elliptic curves [27, 20, 25, 18]. However the problem of finding the maximum gap is interesting on its own and its study can be viewed as a first step toward the detailed understanding of the sparsity structure of Φ_n and Ψ_n .

One can restrict the problem to the case when n is a product of odd primes, because all other cases can be trivially reduced to it (section 2 of [17]). Thus, let us assume that $n = p_1 \cdots p_k$ where $p_1 < \cdots < p_k$ are odd primes. It is obvious that $g(\Phi_{p_1}) = g(\Psi_{p_1}) = 1$. It is also obvious that $g(\Psi_{p_1 p_2}) = p_2 - (p_1 - 1)$. Hence, the simplest non-trivial cases are $g(\Phi_{p_1 p_2})$ and $g(\Psi_{p_1 p_2 p_3})$. In [17], it was shown that $g(\Phi_{p_1 p_2}) = p_1 - 1$ and that $g(\Psi_{p_1 p_2 p_3}) = 2p_2 p_3 - \psi(p_1 p_2 p_3)$ under a certain mild condition, where $\psi(n) = \deg(\Psi_n)$. Since then, several simpler or more insightful proofs were found along with other interesting properties [23, 26, 9].

Naturally, the next challenge is to find general expressions for $g(\Phi_n)$ and $g(\Psi_n)$ where n is the product of an *arbitrary* number of odd primes. However, after several years of attempts, we have not yet found any general expressions, due to combinatorial blowup in the number of cases to consider. Thus, we propose to

consider instead a weaker challenge: find expressions for *lower bounds* of $g(\Phi_n)$ and $g(\Psi_n)$. The weaker challenge is still useful for the original motivation from elliptic curve cryptography.

Thus, in this paper, we tackle the weaker challenge of finding expressions for lower bounds. The main contributions (precisely stated in Section 2) are as follows.

1. We provide four expressions ($\alpha^\pm, \beta^\pm, \gamma^\pm$ and δ^-) for lower bounds (Theorems 1, 2, 3 and 4). These expressions were discovered by carefully inspecting and finding patterns among the maximum gaps of many cyclotomic and inverse cyclotomic polynomials. The four expressions are easy to compute. Furthermore, numerous computer experiments indicate that the combination (maximum) of the four expressions is *very often* exact (Section 4.1).
2. We abstract the four expressions into a single general expression ε^\pm (Theorem 5). The general expression was discovered by observing that each of the four expressions can be rewritten as the difference of two numbers, say u and l , where u is a certain divisor of n and l is a signed sum of several other divisors of n . We also observed that there is indeed a gap between x^l and x^u in the polynomials, which led to an idea for proving the general expression. The general expression takes more time to compute, since it captures many other gaps that are not captured by the four expressions. As a result, ε^\pm is always greater than or equal to $\alpha^\pm, \beta^\pm, \gamma^\pm$ and δ^- . Indeed, numerous computer experiments indicate that it is *almost always* exact (Section 4.2).
3. We provide a sufficient condition that $g(\Psi_n) = \delta^-$ (Theorem 6). It is a straightforward generalization of a result in [17] for the case $k = 3$. We also show that, for every fixed p_1 , the sufficient condition holds “almost always” in a certain sense.
4. Finally we conjecture that $g(\Phi_{p_1 \cdots p_k}) = \varphi(p_1 \cdots p_{k-1})$ if and only if $p_k > p_1 \cdots p_{k-1}$ (Conjecture 7). It is a natural generalization of the result in [17]: $g(\Phi_{p_1 p_2}) = p_1 - 1 = \varphi(p_1)$. The conjecture has been already verified for $m = p_1 \cdots p_{k-1} < 1000$ and arbitrary p_k (Theorem 18). The verification technique is based on a structural result that $g(\Phi_{mp_k})$ only depends on m and $\text{rem}(p_k, m)$ (Theorem 17). Thus, given m , we only need to check finitely many p_k values in order to check the conjecture for infinitely many p_k . We organized it into an algorithm (Algorithm 1) and ran it for all odd square-free $m < 1000$.

The paper is structured as follows: In Section 2, we precisely state the lower bounds and the conjecture informally described above. In Section 3, we illustrate each bound using small examples. In Section 4, we report experimental findings on the quality of the bounds (how often they are exact). In Section 5, we prove the lower bounds. In Section 6, we provide supporting evidence for the conjecture.

2 Main Results

In this section, we precisely state the main results of this paper. From now on, let $n = p_1 \cdots p_k$ where $p_1 < \cdots < p_k$ are odd primes. Recall several standard notations. For a square-free d , $\varphi(d) = \deg(\Phi_d)$, $\psi(d) = \deg(\Psi_d)$, $\omega(d)$ = number of prime factors of d , and $\mu(d) = (-1)^{\omega(d)}$. For an integer i , $\rho(i)$ is the parity, that is $(-1)^i$. We formally define the maximum gap as follows:

Definition 1 (Maximum gap). *Let $f(x) = c_1 x^{\nu_1} + \cdots + c_t x^{\nu_t}$ where $c_1, \dots, c_t \neq 0$ and $0 \leq \nu_1 < \cdots < \nu_t$. Then the maximum gap of f , denoted $g(f)$, is defined as follows*

$$g(f) = \max_{1 \leq i < t} (\nu_{i+1} - \nu_i)$$

if $t \neq 1$, and $g(f) = 0$ if $t = 1$.

Now we are ready to state the four lower bounds for (inverse) cyclotomic polynomials.

Theorem 1 (Special bound α^\pm). *We have $g(\Phi_n) \geq \alpha^+(n)$ and $g(\Psi_n) \geq \alpha^-(n)$ where*

$$\alpha^\pm(n) = \max_{\substack{1 \leq r < k \\ \rho(k-r) = \mp 1}} (p_r - \varphi(p_1 \cdots p_{r-1}))$$

Theorem 2 (Special bound β^\pm). *We have $g(\Phi_n) \geq \beta^+(n)$ and $g(\Psi_n) \geq \beta^-(n)$ where*

$$\beta^\pm(n) = \max_{\substack{1 \leq r < k \\ \rho(k-r) = \mp 1}} (\min \{p_{r+1}, p_1 \cdots p_r\} - \psi(p_1 \cdots p_r))$$

Theorem 3 (Special bound γ^\pm). *We have $g(\Phi_n) \geq \gamma^+(n)$ and $g(\Psi_n) \geq \gamma^-(n)$ where*

$$\gamma^\pm(n) = \max_{\substack{1 \leq r < k \\ \rho(k-r) = \mp 1}} \left(p_1 \cdots p_r - \sum_{\substack{d|n \\ \omega(d) < r}} \pm \mu(n/d) d \right)$$

Theorem 4 (Special bound δ^-). *We have $g(\Psi_n) \geq \delta^-(n)$ where*

$$\delta^-(n) = 2 \frac{n}{p_1} - \psi(n)$$

Now we describe a more general lower bound, which is abstracted from the above four bounds. For this, we need a few notations.

Notation 1. *For a positive integer d and a set B of positive integers, let*

$$\begin{aligned} \bar{d} &= \{h : d \mid h\} & \underline{B} &= \bigcup_{d \in B} \underline{d} \\ \underline{d} &= \{h : h \mid d\} & B^\pm &= \{d \in B : \mu(n/d) = \pm 1\} \end{aligned}$$

Now are ready to state the general bound, unifying the four special bounds.

Theorem 5 (General bound ε^\pm). *We have $g(\Phi_n) \geq \varepsilon^+(n)$ and $g(\Psi_n) \geq \varepsilon^-(n)$ where*

$$\varepsilon^\pm(n) = \max_{\substack{A \uplus B = \underline{n} \setminus \{n\} \\ A \neq \emptyset \\ \mathcal{C}^\pm(B)}} \left(\min A - \sum_{d \in B} \pm \mu(n/d) d \right)$$

where

$$\mathcal{C}^\pm(B) \Leftrightarrow \forall d \in \underline{B} \quad \#(B^\pm \cap \bar{d}) \geq \#(B^\mp \cap \bar{d})$$

Remark 1. *The above four special bounds α^\pm , β^\pm , γ^\pm and δ^- can be obtained from the general bound ε^\pm by considering only certain B 's:*

$$\begin{aligned} \alpha^\pm: B &= \{d : d \mid p_1 \cdots p_{r-1} \text{ and } \omega(d) < r\} & \text{for } 1 \leq r < k \text{ and } \rho(k-r) = \mp 1 \\ \beta^\pm: B &= \{d : d \mid p_1 \cdots p_r \text{ and } \omega(d) < r\} & \text{for } 1 \leq r < k \text{ and } \rho(k-r) = \mp 1 \\ \gamma^\pm: B &= \{d : d \mid p_1 \cdots p_k \text{ and } \omega(d) < r\} & \text{for } 1 \leq r < k \text{ and } \rho(k-r) = \mp 1 \\ \delta^-: B &= \{d : d \mid p_1 \cdots p_k \text{ and } \omega(d) < k \text{ and } d \neq p_2 \cdots p_k\} \end{aligned}$$

It turns out that these B 's satisfy $\mathcal{C}^\pm(B)$.

Theorem 6 (Sufficient condition on $g(\Psi_n)$). *We have*

1. $g(\Psi_n) = \delta^-(n)$ if $\delta^-(n) \geq \frac{1}{2} \frac{n}{p_1}$.
2. For every $k \geq 2$ and every odd prime p , we have

$$\lim_{b \rightarrow \infty} \frac{\#\left\{n : p_k \leq b, p_1 = p, \delta^-(n) \geq \frac{1}{2} \frac{n}{p_1}\right\}}{\#\left\{n : p_k \leq b, p_1 = p\right\}} = 1$$

Conjecture 7 (Equivalent condition on $g(\Phi_n)$). *We have*

$$g(\Phi_n) = \varphi(p_1 \cdots p_{k-1}) \text{ if and only if } p_k > p_1 \cdots p_{k-1}$$

3 Examples

3.1 Examples for the bound $\alpha^\pm, \beta^\pm, \gamma^\pm, \delta^-$ and ε^\pm (Theorems 1, 2, 3, 4 and 5)

In the following two tables, we give the values of $g(\Phi_n)$, $g(\Psi_n)$ and the lower bounds on several values of n .

n	$3 \cdot 5 \cdot 11 \cdot 13$	$3 \cdot 5 \cdot 7 \cdot 71$	$7 \cdot 11 \cdot 13 \cdot 17$	$3 \cdot 7 \cdot 11 \cdot 13$	$3 \cdot 5 \cdot 7 \cdot 11$
$g(\Phi_n)$	3	14	210	17	10
$\alpha^+(n)$	3	2	6	2	2
$\beta^+(n)$	2	14	6	2	2
$\gamma^+(n)$	2	2	210	2	2
$\varepsilon^+(n)$	3	14	210	17	2

n	$5 \cdot 7 \cdot 11 \cdot 13$	$7 \cdot 11 \cdot 13 \cdot 17$	$3 \cdot 5 \cdot 7 \cdot 11$	$7 \cdot 11 \cdot 13 \cdot 41$	$7 \cdot 11 \cdot 13$
$g(\Psi_n)$	3	30	95	11	7
$\alpha^-(n)$	3	5	3	5	6
$\beta^-(n)$	0	-4	0	4	6
$\gamma^-(n)$	0	30	-10	6	6
$\delta^-(n)$	-123	-635	95	-515	5
$\varepsilon^-(n)$	3	30	95	11	6

In the above tables, we marked the exact ones in boldface, that is, the ones that match $g(\Phi_n)$ or $g(\Psi_n)$. For the last column, we chose the smallest n such that $g(\Phi_n)$ and $g(\Psi_n)$ is not equal to any of the lower bounds. After checking all the values of $n < 15013$, we have not found any such example for the cyclotomic case where $k = 3$.

In the following, we will illustrate how the above bounds are computed for some of the examples.

Example 1 (α^+). Let $n = 3 \cdot 5 \cdot 11 \cdot 13$. We will compute $\alpha^+(n)$. Let

$$u = p_r$$

$$l = \varphi(p_1 \cdots p_{r-1})$$

The following table shows the values of $u - l$ for all choices of r such that $1 \leq r < k$ and $\delta(k - r) = -1$.

r	u	l	$u - l$
1	3	1	2
3	11	8	3

Thus $\alpha^+(n) = 3$.

Example 2 (β^+). Let $n = 3 \cdot 5 \cdot 7 \cdot 71$. We will compute $\beta^+(n)$. Let

$$u = \min \{p_{r+1}, p_1 \cdots p_r\}$$

$$l = \psi(p_1 \cdots p_r)$$

The following table shows the values of $u - l$ for all choices of r such that $1 \leq r < k$ and $\delta(k - r) = -1$.

r	u	l	$u - l$
1	3	1	2
3	71	57	14

Thus $\beta^+(n) = 14$.

Example 3 (γ^+). Let $n = 7 \cdot 11 \cdot 13 \cdot 17$. We will compute $\gamma^+(n)$. Let

$$u = p_1 \cdots p_r$$

$$B = \{d : d \mid n \text{ and } \omega(d) < r\}$$

$$l = \sum_{d \in B} \mu(n/d) d$$

The following table shows the values of $u - l$ for all choices of r such that $1 \leq r < k$ and $\delta(k - r) = -1$.

r	u	B	l	$u - l$
1	7	$\{1\}$	1	6
3	$7 \cdot 11 \cdot 13$	$\{1, 7, 11, 13, 17, 77, 91, 119, 143, 187, 221\}$	791	210

Thus $\gamma^+(n) = 210$.

Example 4 (ε^+). Let $n = 3 \cdot 7 \cdot 11 \cdot 13$. We will compute $\varepsilon^+(n)$. Let

$$u = \min A$$

$$l = \sum_{d \in B} \mu(n/d) d$$

The following table shows the values of $u - l$ for some A and B such that $A \uplus B = \underline{n} \setminus \{n\}$, $A \neq \emptyset$, and $C^+(B)$. There are 1566 such pairs of A and B , so we only list a few below.

A	B	u	l	$u - l$
$\{3, 7, 11, 13, 3 \cdot 7, \dots\}$	$\{1\}$	3	1	2
$\{11, 13, 3 \cdot 11, 3 \cdot 13, 7 \cdot 11, \dots\}$	$\{1, 3, 7, 3 \cdot 7\}$	11	12	-1
$\{13, 3 \cdot 13, 7 \cdot 11, 7 \cdot 13, \dots\}$	$\{1, 3, 7, 11, 3 \cdot 7, 3 \cdot 11\}$	13	34	-21
$\{7 \cdot 11, 7 \cdot 13, 11 \cdot 13, \dots\}$	$\{1, 3, 7, 11, 13, 3 \cdot 7, 3 \cdot 11, 3 \cdot 13\}$	$7 \cdot 11$	60	17
\dots	\dots			

Thus $\varepsilon^+(n) = 17$.

Example 5 (α^-). Let $n = 5 \cdot 7 \cdot 11 \cdot 13$. We will compute $\alpha^-(n)$. Let

$$u = p_r$$

$$l = \varphi(p_1 \cdots p_{r-1})$$

The following table shows the values of $u - l$ for all choices of r such that $1 \leq r < k$ and $\delta(k - r) = +1$.

r	u	l	$u - l$
2	7	4	3

Thus $\alpha^-(n) = 3$.

Example 6 (γ^-). Let $n = 7 \cdot 11 \cdot 13 \cdot 17$. We will compute $\gamma^-(n)$. Let

$$u = p_1 \cdots p_r$$

$$B = \{d : d \mid n \text{ and } \omega(d) < r\}$$

$$l = \sum_{d \in B} -\mu(n/d) d$$

The following table shows the values of $u - l$ for all choices of r such that $1 \leq r < k$ and $\delta(k - r) = +1$.

r	u	B	l	$u - l$
2	$7 \cdot 11$	$\{1, 7, 11, 13, 17\}$	47	30

Thus $\gamma^-(n) = 30$.

Example 7 (δ^-). Let $n = 3 \cdot 5 \cdot 7$. We will compute $\delta^-(n)$. Note

$$\begin{aligned}\delta^-(n) &= 2 \frac{n}{p_1} - \psi(n) \\ &= 2 \frac{3 \cdot 5 \cdot 7}{3} - (3 \cdot 5 \cdot 7 - (3 - 1)(5 - 1)(7 - 1)) \\ &= 13\end{aligned}$$

Thus $\delta^-(n) = 13$.

Example 8 (ε^-). Let $n = 7 \cdot 11 \cdot 13 \cdot 41$. We will compute $\varepsilon^-(n)$. Let

$$\begin{aligned}u &= \min A \\ l &= \sum_{d \in B} -\mu(n/d) d\end{aligned}$$

The following table shows the values of $u - l$ for some A and B such that $A \uplus B = \underline{n} \setminus \{n\}$, $A \neq \emptyset$, and $C^-(B)$. There are 13301 such pairs of A and B , so we only list a few below.

A	B	u	l	$u - l$
$\{11, 13, 41, 7 \cdot 11, 7 \cdot 13, \dots\}$	$\{1, 7\}$	11	6	5
$\{1, 41, 7 \cdot 11, 7 \cdot 13, 11 \cdot 13, \dots\}$	$\{7, 11, 13\}$	1	31	-30
$\{41, 7 \cdot 11, 7 \cdot 13, 11 \cdot 13, \dots\}$	$\{1, 7, 11, 13\}$	41	30	11
\dots	\dots			

Thus $\varepsilon^-(n) = 11$.

3.2 Examples for Sufficient condition on $g(\Psi_n)$ (Theorem 6)

Example 9. Let $n = 3 \cdot 7 \cdot 11$. Then $\delta^-(n) = 43$. Consider

$$\frac{1}{2} \left(\frac{3 \cdot 7 \cdot 11}{3} \right) = \frac{77}{2} \leq \delta^-(n)$$

Computation of Ψ_n shows that $g(\Psi_n) = 43$, as expected from the theorem.

Example 10. Let $n = 3 \cdot 5 \cdot 7$. In Example 7 we showed that $\delta^-(n) = 13$ and $g(\Psi_n) = 13$. Consider the following

$$\frac{1}{2} \left(\frac{3 \cdot 5 \cdot 7}{3} \right) = \frac{35}{2} > \delta^-(n)$$

Therefore, the condition is sufficient but not necessary.

Example 11. Let $n = 7 \cdot 11 \cdot 13$. Then $\delta^-(n) = 5$. Consider

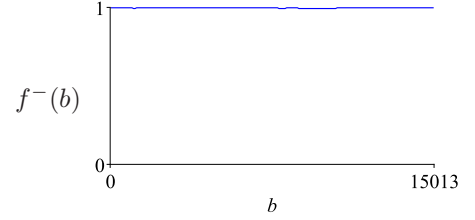
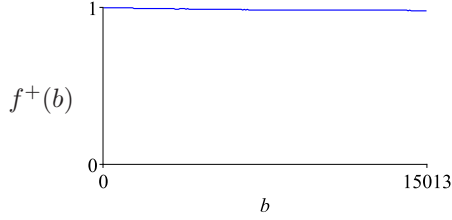
$$\frac{1}{2} \left(\frac{7 \cdot 11 \cdot 13}{7} \right) = \frac{143}{2} > \delta^-(n)$$

Computation of Ψ_n shows that $g(\Psi_n) = 6$. Thus $\delta^-(n) \neq g(\Psi_n)$.

4 Quality

4.1 Quality of Special bounds α^\pm , β^\pm , γ^\pm and δ^- (Theorems 1, 2, 3 and 4)

The following graphs show how often the lower bound is equal to the maximum gap.



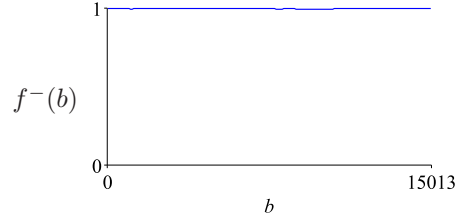
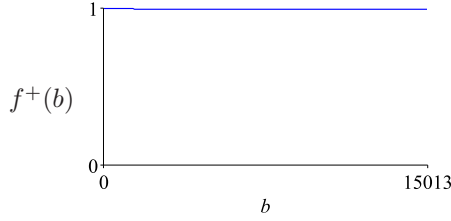
$$f^+(b) = \frac{\#\{n < b : g(\Phi_n) = \max\{\alpha^+(n), \beta^+(n), \gamma^+(n)\}\}}{\#\{n < b\}}$$

$$f^-(b) = \frac{\#\{n < b : g(\Psi_n) = \max\{\alpha^-(n), \beta^-(n), \gamma^-(n), \delta^-(n)\}\}}{\#\{n < b\}}$$

In the above graphs, $f^+(15013) = 0.9829$ and $f^-(15013) = 0.9984$.

4.2 Quality of General bound ε^\pm (Theorem 5)

The following graphs show how often the lower bound is equal to the maximum gap.



$$f^+(b) = \frac{\#\{n < b : g(\Phi_n) = \varepsilon^+(n)\}}{\#\{n < b\}}$$

$$f^-(b) = \frac{\#\{n < b : g(\Psi_n) = \varepsilon^-(n)\}}{\#\{n < b\}}$$

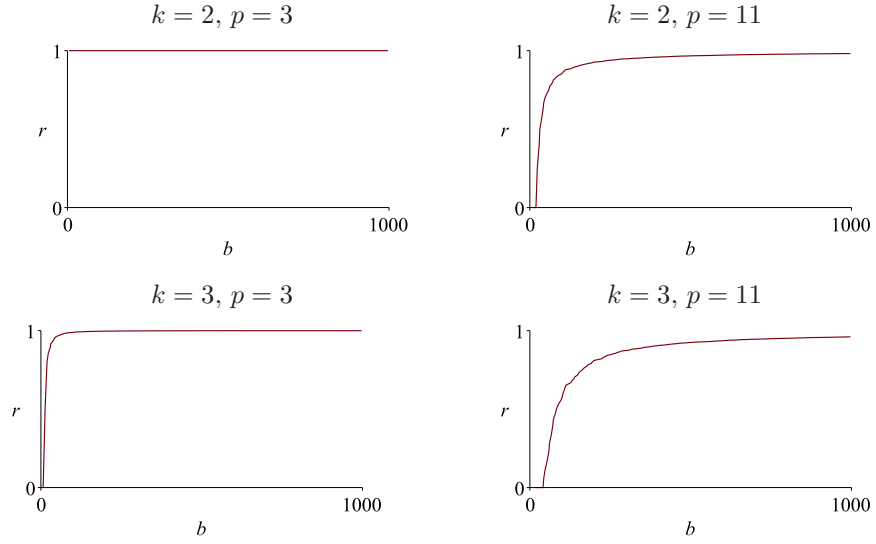
In the above graphs, $f^+(15013) = 0.9957$ and $f^-(15013) = 0.9984$.

4.3 Quality of Sufficient condition on $g(\Psi_n)$ (Theorem 6)

The following plots show the following ratio for various values of k and p .

$$r = \frac{\#\left\{n : p_k \leq b, p_1 = p, \delta^-(n) \geq \frac{1}{2} \frac{n}{p_1}\right\}}{\#\{n : p_k \leq b, p_1 = p\}}$$

We observe that in all cases, the ratio goes to 1, as expected from the theorem.



5 Proof

In this section, we prove the main results (Theorems 1, 2, 3, 4, 5 and 6). We will first prove the general lower bound ε^\pm (Theorem 5). Then we will prove the other four special lower bounds α^\pm , β^\pm , γ^\pm and δ^- (Theorems 1, 2, 3 and 4) as certain restrictions of Theorem 5. After that, we will prove the sufficient condition on $g(\Psi_n)$ (Theorem 6). In order to simplify the presentation of the proof, we introduce some notations.

Notation 2.

$$n_r = p_1 \cdots p_r \quad u(A) = \min A \quad l^\pm(B) = \sum_{d \in B} \pm \mu(n/d) \quad d$$

5.1 Proof of General bound ε^\pm (Theorem 5)

We divide the proof into several lemmas.

Notation 3. Let

$$F_C := \prod_{c \in C} (x^c - 1)$$

and $F(C) = 1$ if $C = \emptyset$.

Lemma 8. We have that $\frac{F_{B^\pm}}{F_{B^\mp}}$ is a polynomial if

$$\mathcal{C}^\pm(B) = \text{true} \\ B \subset \underline{n}$$

Proof. Let $C \subset \underline{n}$. Consider the following equalities.

$$F_C = \prod_{c \in C} (x^c - 1) = \prod_{c \in C} \prod_{d|c} \Phi_d = \prod_{d \in \underline{n}} \prod_{\substack{c \in C \\ d|c}} \Phi_d = \prod_{d \in \underline{n}} \Phi_d^{\#\{c \in C : d|c\}} = \prod_{d \in \underline{n}} \Phi_d^{\#(C \cap \overline{d})}$$

Thus

$$\frac{F_{B^\pm}}{F_{B^\mp}} = \frac{\prod_{d \in \underline{n}} \Phi_d^{\#(B^\pm \cap \bar{d})}}{\prod_{d \in \underline{n}} \Phi_d^{\#(B^\mp \cap \bar{d})}} = \prod_{d \in \underline{n}} \Phi_d^{\#(B^\pm \cap \bar{d}) - \#(B^\mp \cap \bar{d})}$$

Note that for $d \in \underline{n} \setminus \underline{B}$, we have $\#(B^+ \cap \bar{d}) = 0$ and $\#(B^- \cap \bar{d}) = 0$. Thus,

$$\frac{F_{B^\pm}}{F_{B^\mp}} = \prod_{d \in \underline{B}} \Phi_d^{\#(B^\pm \cap \bar{d}) - \#(B^\mp \cap \bar{d})}$$

Recall $\mathcal{C}^\pm(B) \iff \forall d \in \underline{B} \ \#(B^\pm \cap \bar{d}) \geq \#(B^\mp \cap \bar{d})$. Therefore, $\frac{F_{B^\pm}}{F_{B^\mp}}$ is a polynomial. \square

Lemma 9. *We have*

$$P^\pm \equiv_{x^{u(A)+1}} \pm \begin{cases} -(-1)^{|A|} G^\pm - x^{u(A)} & \text{if } u(A) \in A^\pm \\ -(-1)^{|A|} G^\pm + x^{u(A)} & \text{if } u(A) \in A^\mp \end{cases}$$

where

$$\begin{aligned} P^\pm &= \frac{F_{\underline{n}^\pm} F_{\{n\}^\mp}}{F_{\underline{n}^\mp}} \\ G^\pm &= \frac{F_{B^\pm}}{F_{B^\mp}} \\ A \uplus B &= \underline{n} \setminus \{n\} \\ A &\neq \emptyset \\ \mathcal{C}^\pm(B) &= \text{true} \\ |B| &= \#\{b \in B\} \end{aligned}$$

and the notation $\square \equiv_{x^{u(A)+1}} \triangle$ stands for $x^{u(A)+1} | \square - \triangle$.

Proof. For simplicity, in the rest of this proof we will use u instead of $u(A)$. Since $A \neq \emptyset$, $u(A)$ is defined. Note

$$\begin{aligned} F_{\underline{n}^\mp} P^\pm &= F_{\underline{n}^\pm} F_{\{n\}^\mp} \\ F_{\{n\}^\mp} F_{A^\mp} F_{B^\mp} P^\pm &= F_{A^\pm} F_{B^\pm} F_{\{n\}^\pm} F_{\{n\}^\mp} \end{aligned}$$

Case: $u \in A^\pm$. Since $u = \min A$ we have

$$\begin{aligned} F_{A^\pm \setminus \{u\}} &\equiv_{x^{u+1}} (-1)^{|A^\pm|-1} \\ F_{A^\mp} &\equiv_{x^{u+1}} (-1)^{|A^\mp|} \\ F_{\{n\}^\pm} &\equiv_{x^{u+1}} (-1)^{|\{n\}^\pm|} \\ F_{\{n\}^\mp} &\equiv_{x^{u+1}} (-1)^{|\{n\}^\mp|} \end{aligned}$$

Thus

$$F_{B^\mp} P^\pm \equiv_{x^{u+1}} (-1)^{|A|-1+|\{n\}^\pm|} (x^u - 1) F_{B^\pm}$$

Since $\mathcal{C}^\pm(B)$, by Lemma 8 we have

$$F_{B^\mp} P^\pm \equiv_{x^{u+1}} (-1)^{|A|-1+|\{n\}^\pm|} (x^u - 1) F_{B^\mp} G^\pm$$

Note that 0 is the only root of x^{u+1} and $F_{B^\mp}(0) = (-1)^{|B^\mp|}$. Hence $\gcd(F_{B^\mp}, x^{u+1}) = 1$. Thus we can cancel F_{B^\mp} from both sides, obtaining

$$P^\pm \equiv_{x^{u+1}} (-1)^{|A|-1+|\{n\}^\pm|} (x^u - 1) G^\pm$$

$$\equiv_{x^{u+1}} -(-1)^{|A|-1+|\{n\}^\pm|} G^\pm + (-1)^{|A|-1+|\{n\}^\pm|} x^u G^\pm$$

Note that $G^\pm(0) = (-1)^{|B|}$. Thus we have

$$\begin{aligned} P^\pm &\equiv_{x^{u+1}} -(-1)^{|A|-1+|\{n\}^\pm|} G^\pm + (-1)^{|A|-1+|\{n\}^\pm|+|B|} x^u \\ &\equiv_{x^{u+1}} (-1)^{-1+|\{n\}^\pm|} \left(-(-1)^{|A|} G^\pm + (-1)^{|A|+|B|} x^u \right) \\ &\equiv_{x^{u+1}} \pm \left(-(-1)^{|A|} G^\pm + (-1)^{2^k-1} x^u \right) \\ &\equiv_{x^{u+1}} \pm \left(-(-1)^{|A|} G^\pm - x^u \right) \end{aligned}$$

which proves the lemma.

Case: $u \in A^\mp$. Since $u = \min A$ we have

$$\begin{aligned} F_{A^\pm} &\equiv_{x^{u+1}} (-1)^{|A^\pm|} \\ F_{A^\mp \setminus \{u\}} &\equiv_{x^{u+1}} (-1)^{|A^\mp|-1} \\ F_{\{n\}^\pm} &\equiv_{x^{u+1}} (-1)^{|\{n\}^\pm|} \\ F_{\{n\}^\mp} &\equiv_{x^{u+1}} (-1)^{|\{n\}^\mp|} \end{aligned}$$

Thus

$$(x^u - 1) F_{B^\mp} \cdot P^\pm \equiv_{x^{u+1}} (-1)^{|A|-1+|\{n\}^\pm|} F_{B^\pm}$$

Since $\mathcal{C}^\pm(B)$, by Lemma 8 we have

$$(x^u - 1) F_{B^\mp} \cdot P^\pm \equiv_{x^{u+1}} (-1)^{|A|-1+|\{n\}^\pm|} F_{B^\mp} \cdot G^\pm$$

Note that 0 is the only root of x^{u+1} and $F_{B^\mp}(0) = (-1)^{|B^\mp|}$. Hence $\gcd(F_{B^\mp}, x^{u+1}) = 1$. Thus we can cancel F_{B^\mp} from both sides, obtaining

$$(x^u - 1) P^\pm \equiv_{x^{u+1}} (-1)^{|A|-1+|\{n\}^\pm|} G^\pm$$

Multiplying both sides by $(x^u + 1)$, we have

$$\begin{aligned} (x^u + 1)(x^u - 1) P^\pm &\equiv_{x^{u+1}} (x^u + 1)(-1)^{|A|-1+|\{n\}^\pm|} G^\pm \\ (x^{2u} - 1) P^\pm &\equiv_{x^{u+1}} (-1)^{|A|-1+|\{n\}^\pm|} G^\pm + (-1)^{|A|-1+|\{n\}^\pm|} x^u G^\pm \\ -P^\pm &\equiv_{x^{u+1}} (-1)^{|A|-1+|\{n\}^\pm|} G^\pm + (-1)^{|A|-1+|\{n\}^\pm|} x^u G^\pm \\ P^\pm &\equiv_{x^{u+1}} -(-1)^{|A|-1+|\{n\}^\pm|} G^\pm - (-1)^{|A|-1+|\{n\}^\pm|} x^u G^\pm \end{aligned}$$

Note that $G^\pm(0) = (-1)^{|B|}$. Thus we have

$$\begin{aligned} P^\pm &\equiv_{x^{u+1}} -(-1)^{|A|-1+|\{n\}^\pm|} G^\pm - (-1)^{|A|-1+|\{n\}^\pm|+|B|} x^u \\ &\equiv_{x^{u+1}} (-1)^{-1+|\{n\}^\pm|} \left(-(-1)^{|A|} G^\pm - (-1)^{|A|+|B|} x^u \right) \\ &\equiv_{x^{u+1}} \pm \left(-(-1)^{|A|} G^\pm - (-1)^{2^k-1} x^u \right) \\ &\equiv_{x^{u+1}} \pm \left(-(-1)^{|A|} G^\pm + x^u \right) \end{aligned}$$

which proves the lemma. □

Proof of Theorem 5-(1). Using the same notation as in Lemma 9, note

$$P^+ = \Phi_n$$

Let A and B be such that $A \uplus B = \underline{n} \setminus \{n\}$, $A \neq \emptyset$, and $\mathcal{C}^+(B)$. By Lemma 9, we have

$$\Phi_n = + \begin{cases} -(-1)^{|A|} G^+ - x^{u(A)} + x^{u(A)+1} H & \text{if } u(A) \in A^+ \\ -(-1)^{|A|} G^+ + x^{u(A)} + x^{u(A)+1} H & \text{if } u(A) \in A^- \end{cases}$$

for some polynomial H . Note

$$\deg G^+ = \deg \left(\frac{F_{B^+}}{F_{B^-}} \right) = \sum_{d \in B^+} d - \sum_{d \in B^-} d = \sum_{d \in B} \mu(n/d) d = l^+(B)$$

If $u(A) \leq l^+(B)$, then clearly

$$g(\Phi_n) \geq u(A) - l^+(B)$$

If $u(A) > l^+(B)$, then $x^{l^+(B)}$ and $x^{u(A)}$ appear in Φ_n , so we have

$$g(\Phi_n) \geq u(A) - l^+(B)$$

Thus

$$g(\Phi_n) \geq \max_{\substack{A \uplus B = \underline{n} \setminus \{n\} \\ A \neq \emptyset \\ \mathcal{C}^+(B)}} u(A) - l^+(B) = \varepsilon^+(n)$$

The theorem has been proved. □

Proof of Theorem 5-(2). Using the same notation as in Lemma 9, note

$$P^- = \Psi_n$$

Let A and B be such that $A \uplus B = \underline{n} \setminus \{n\}$, $A \neq \emptyset$, and $\mathcal{C}^-(B)$. By Lemma 9, we have

$$\Psi_n = - \begin{cases} -(-1)^{|A|} G^- - x^{u(A)} + x^{u(A)+1} H & \text{if } u(A) \in A^- \\ -(-1)^{|A|} G^- + x^{u(A)} + x^{u(A)+1} H & \text{if } u(A) \in A^+ \end{cases}$$

for some polynomial H . Note

$$\deg G^- = \deg \left(\frac{F_{B^-}}{F_{B^+}} \right) = \sum_{d \in B^-} d - \sum_{d \in B^+} d = \sum_{d \in B} -\mu(n/d) d = l^-(B)$$

If $u(A) \leq l^-(B)$, then clearly

$$g(\Psi_n) \geq u(A) - l^-(B)$$

If $u(A) > l^-(B)$, then $x^{l^-(B)}$ and $x^{u(A)}$ appear in Ψ_n , so we have

$$g(\Psi_n) \geq u(A) - l^-(B)$$

Thus

$$g(\Psi_n) \geq \max_{\substack{A \uplus B = \underline{n} \setminus \{n\} \\ A \neq \emptyset \\ \mathcal{C}^-(B)}} u(A) - l^-(B) = \varepsilon^-(n)$$

The theorem has been proved. □

5.2 Proof of Special bounds α^\pm , β^\pm and γ^\pm (Theorems 1, 2 and 3)

We restrict the choice of B as mentioned in Section 2. Note that the restrictions are very similar. To deal with them at the same time, we will use the following uniform notation

$$\Omega_{jr} = \left\{ c \in \underline{n_j} : \omega(c) < r \right\}$$

Note that B for α^\pm , β^\pm and γ^\pm can be compactly written as $B = \Omega_{r-1,r}$, $B = \Omega_{rr}$ and $B = \Omega_{kr}$ respectively. In the following three lemmas, we will show that $\mathcal{C}^\pm(\Omega_{jr})$ holds.

Lemma 10. *We have, for $s \in \{+, -\}$, that*

$$\#(\Omega_{jr}^s \cap \overline{d}) = \sum_{\substack{0 \leq i < r - \omega(d) \\ \rho(i) = s\rho(k - \omega(d))}} \binom{j - \omega(d)}{i}$$

for $1 \leq r < k$, $r - 1 \leq j \leq k$ and $d \in \underline{\Omega_{jr}}$.

Proof. Note

$$\begin{aligned} \#(\Omega_{jr}^s \cap \overline{d}) &= \#\{c \in \underline{n_j} : \omega(c) < r, \quad \mu(n/c) = s, d \mid c\} \\ &= \#\{ld \in \underline{n_j} : \omega(ld) < r, \quad \mu(n/(ld)) = s\} \\ &= \#\{l \in \underline{n_j/d} : \omega(l) < r - \omega(d), \quad \mu(l) = s\mu(n/d)\} \end{aligned}$$

Note

$$s\mu(n/d) = s\rho(k - \omega(d))$$

Thus

$$\begin{aligned} \#(\Omega_{jr}^s \cap \overline{d}) &= \# \bigsqcup_{\substack{0 \leq i < r - \omega(d) \\ \rho(i) = s\rho(k - \omega(d))}} \{l \in \underline{n_j/d} : \omega(l) = i\} \\ &= \sum_{\substack{0 \leq i < r - \omega(d) \\ \rho(i) = s\rho(k - \omega(d))}} \#\{l \in \underline{n_j/d} : \omega(l) = i\} \\ &= \sum_{\substack{0 \leq i < r - \omega(d) \\ \rho(i) = s\rho(k - \omega(d))}} \binom{\omega(n_j/d)}{i} \\ &= \sum_{\substack{0 \leq i < r - \omega(d) \\ \rho(i) = s\rho(k - \omega(d))}} \binom{j - \omega(d)}{i} \end{aligned}$$

which proves the lemma. □

Lemma 11 (Telescoping sum). *We have*

$$\sum_{0 \leq i \leq u} \rho(i) \binom{t}{i} = \begin{cases} \rho(u) \binom{t-1}{u} & \text{if } t \geq 1 \\ 1 & \text{if } t = 0 \end{cases}$$

Proof. When $t \geq 1$, we have

$$\sum_{0 \leq i \leq u} \rho(i) \binom{t}{i} = \sum_{0 \leq i \leq u} \rho(i) \binom{t-1}{i-1} + \sum_{0 \leq i \leq u} \rho(i) \binom{t-1}{i}$$

$$\begin{aligned}
&= - \sum_{-1 \leq i \leq u-1} \rho(i) \binom{t-1}{i} + \sum_{0 \leq i \leq u} \rho(i) \binom{t-1}{i} \\
&= -\rho(-1) \binom{t-1}{-1} + \rho(u) \binom{t-1}{u} \\
&= \rho(u) \binom{t-1}{u}
\end{aligned}$$

When $t = 0$, we have

$$\sum_{0 \leq i \leq u} \rho(i) \binom{t}{i} = \rho(0) \binom{0}{0} + \sum_{1 \leq i \leq u} \rho(i) \binom{0}{i} = 1 + 0 = 1$$

□

Lemma 12. We have $\mathcal{C}^\pm(\Omega_{jr})$ for $1 \leq r < k$, $\rho(k-r) = \mp 1$ and $r-1 \leq j \leq k$.

Proof. Recall

$$\mathcal{C}^\pm(\Omega_{jr}) \iff \forall d \in \underline{\Omega_{jr}} \quad \#(\Omega_{jr}^\pm \cap \bar{d}) \geq \#(\Omega_{jr}^\mp \cap \bar{d})$$

Note

$$\begin{aligned}
&\#(\Omega_{jr}^\pm \cap \bar{d}) - \#(\Omega_{jr}^\mp \cap \bar{d}) \\
&= \sum_{\substack{0 \leq i < r-\omega(d) \\ \rho(i) = \pm \rho(k-\omega(d))}} \binom{j-\omega(d)}{i} - \sum_{\substack{0 \leq i < r-\omega(d) \\ \rho(i) = \mp \rho(k-\omega(d))}} \binom{j-\omega(d)}{i} \quad \text{by Lemma 10} \\
&= \sum_{\substack{0 \leq i < r-\omega(d) \\ \rho(i) = -\rho(k-r)\rho(k-\omega(d))}} \binom{j-\omega(d)}{i} - \sum_{\substack{0 \leq i < r-\omega(d) \\ \rho(i) = +\rho(k-r)\rho(k-\omega(d))}} \binom{j-\omega(d)}{i} \quad \text{since } \rho(k-r) = \mp 1 \\
&= \sum_{\substack{0 \leq i < r-\omega(d) \\ \rho(i) = -\rho(r-\omega(d))}} \binom{j-\omega(d)}{i} - \sum_{\substack{0 \leq i < r-\omega(d) \\ \rho(i) = +\rho(r-\omega(d))}} \binom{j-\omega(d)}{i} \\
&= \sum_{0 \leq i < r-\omega(d)} -\rho(r-\omega(d)) \rho(i) \binom{j-\omega(d)}{i} \\
&= -\rho(r-\omega(d)) \sum_{0 \leq i < r-\omega(d)} \rho(i) \binom{j-\omega(d)}{i} \\
&= -\rho(r-\omega(d)) \begin{cases} \rho(r-\omega(d)-1) \binom{j-\omega(d)-1}{r-\omega(d)-1} & \text{if } j-\omega(d) \geq 1 \\ 1 & \text{if } j-\omega(d) = 0 \end{cases} \quad \text{by Lemma 11} \\
&= \begin{cases} -\rho(r-\omega(d)) \rho(r-\omega(d)-1) \binom{j-\omega(d)-1}{r-\omega(d)-1} & \text{if } j-\omega(d) \geq 1 \\ -\rho(r-\omega(d)) & \text{if } j-\omega(d) = 0 \end{cases} \\
&= \begin{cases} \binom{j-\omega(d)-1}{r-\omega(d)-1} & \text{if } j-\omega(d) \geq 1 \\ -\rho(r-\omega(d)) & \text{if } j-\omega(d) = 0 \end{cases}
\end{aligned}$$

Consider the case $j - \omega(d) = 0$: Since $r-1 \leq j = \omega(d) \leq r-1$, we have $\omega(d) = r-1$. Therefore we have

$$\#(\Omega_{jr}^\pm \cap \bar{d}) - \#(\Omega_{jr}^\mp \cap \bar{d}) = \begin{cases} \binom{j-\omega(d)-1}{r-\omega(d)-1} & \text{if } j-\omega(d) \geq 1 \\ -\rho(1) & \text{if } j-\omega(d) = 0 \end{cases}$$

$$= \begin{cases} \binom{j-\omega(d)-1}{r-\omega(d)-1} & \text{if } j - \omega(d) \geq 1 \\ 1 & \text{if } j - \omega(d) = 0 \end{cases} \geq 0$$

which proves the lemma. \square

Lemma 13. *We have, for $r - 1 \leq j \leq k$,*

$$\varepsilon^\pm(n) \geq \max_{\substack{1 \leq r < k \\ \rho(k-r)=\mp 1}} \left(\min \{p_{j+1}, n_r\} - \sum_{\substack{d|n_j \\ \omega(d) < r}} \pm \mu(n/d) d \right)$$

where p_{k+1} is viewed as ∞ .

Proof. Note

$$\begin{aligned} \varepsilon^\pm(n) &= \max_{\substack{A \uplus B = \underline{n} \setminus \{n\} \\ A \neq \emptyset \\ \mathcal{C}^\pm(B)}} u(A) - l^\pm(B) \\ &\geq \max_{\substack{A \uplus B = \underline{n} \setminus \{n\} \\ A \neq \emptyset \\ \mathcal{C}^\pm(B) \\ 1 \leq r < k \\ \rho(k-r)=\mp 1 \\ B = \Omega_{jr}}} u(A) - l^\pm(B) \quad \text{by restricting the choice of } B \text{ to } \Omega_{jr} \\ &= \max_{\substack{1 \leq r < k \\ \rho(k-r)=\mp 1 \\ \mathcal{C}^\pm(\Omega_{jr})}} u(\underline{n} \setminus \{n\} \setminus \Omega_{jr}) - l^\pm(\Omega_{jr}) \\ &= \max_{\substack{1 \leq r < k \\ \rho(k-r)=\mp 1}} u(\underline{n} \setminus \{n\} \setminus \Omega_{jr}) - l^\pm(\Omega_{jr}) \quad \text{by Lemma 12} \end{aligned}$$

Note

$$\begin{aligned} u(\underline{n} \setminus \{n\} \setminus \Omega_{jr}) &= \min(\underline{n} \setminus \{n\} \setminus \Omega_{jr}) \\ &= \min(\underline{n} \setminus \{n\} \setminus \{c : c|n_j, \omega(c) < r\}) \\ &= \min\{c : c|n, c \neq n \text{ and } (c \nmid n_j \text{ or } \omega(c) \geq r)\} \\ &= \min(\min\{c : c|n, c \neq n \text{ and } c \nmid n_j\}, \min\{c : c|n, c \neq n \text{ and } \omega(c) \geq r\}) \\ &= \min\left(\min\left\{c : c|n, c \neq n \text{ and } \exists_{i \geq j+1} p_i | c\right\}, n_r\right) \\ &= \min\{p_{j+1}, n_r\} \end{aligned}$$

Note

$$l^\pm(\Omega_{jr}) = \sum_{d \in \Omega_{jr}} \pm \mu(n/d) d = \sum_{\substack{d \in \underline{n_j} \\ \omega(d) < r}} \pm \mu(n/d) d$$

Hence

$$\varepsilon^\pm(n) \geq \max_{\substack{1 \leq r < k \\ \rho(k-r)=\mp 1}} \left(\min \{p_{j+1}, n_r\} - \sum_{\substack{d \in \underline{n_j} \\ \omega(d) < r}} \pm \mu(n/d) d \right)$$

\square

Lemma 14. *We have*

$$\varphi(n_r) = \sum_{d|n_r} \mu(n_r/d) d$$

Proof. Note

$$\varphi(n_r) = (p_1 - 1) \cdots (p_r - 1) = (-1)^r (1 - p_1) \cdots (1 - p_r) = (-1)^r \sum_{d|n_r} \mu(d) d = \sum_{d|n_r} \mu(n_r/d) d$$

□

Proof of Theorem 1. We set $j = r - 1$. Note

$$\varepsilon^\pm(n) \geq \max_{\substack{1 \leq r < k \\ \rho(k-r) = \mp 1}} \left(\min \{p_{r-1+1}, n_r\} - \sum_{\substack{d|n_{r-1} \\ \omega(d) < r}} \pm \mu(n/d) d \right) \quad \text{by Lemma 13}$$

Note that

$$\min \{p_{r-1+1}, n_r\} = \min \{p_r, n_r\} = p_r$$

Not that

$$\begin{aligned} \sum_{\substack{d|n_{r-1} \\ \omega(d) < r}} \pm \mu(n/d) d &= \sum_{d|n_{r-1}} \pm \mu(n/d) d \\ &= \sum_{d|n_{r-1}} \pm \mu(n/n_{r-1}) \mu(n_{r-1}/d) d \\ &= \sum_{d|n_{r-1}} \pm 1 \cdot \pm 1 \mu(n_{r-1}/d) d \\ &= \sum_{d|n_{r-1}} \mu(n_{r-1}/d) d \\ &= \varphi(n_{r-1}) \quad \text{by Lemma 14} \end{aligned}$$

Thus

$$\varepsilon^\pm(n) \geq \max_{\substack{1 \leq r < k \\ \rho(k-r) = \mp 1}} (p_r - \varphi(n_{r-1})) = \max_{\substack{1 \leq r < k \\ \rho(k-r) = \mp 1}} (p_r - \varphi(p_1 \cdots p_{r-1})) = \alpha^\pm(n)$$

Hence

$$\begin{aligned} g(\Phi_n) &\geq \varepsilon^+(n) \geq \alpha^+(n) \\ g(\Psi_n) &\geq \varepsilon^-(n) \geq \alpha^-(n) \end{aligned}$$

The theorem has been proved. □

Proof of Theorem 2. We set $j = r$. Note

$$\varepsilon^\pm(n) \geq \max_{\substack{1 \leq r < k \\ \rho(k-r) = \mp 1}} \left(\min \{p_{r+1}, n_r\} - \sum_{\substack{d \in \underline{n_r} \\ \omega(d) < r}} \pm \mu(n/d) d \right) \quad \text{by Lemma 13}$$

Note that

$$\sum_{\substack{d \in \underline{n_r} \\ \omega(d) < r}} \pm \mu(n/d) d = \sum_{d \in \underline{n_r} \setminus \{n_r\}} \pm \mu(n/n_r) \mu(n_r/d) d$$

$$\begin{aligned}
&= \sum_{d \in \underline{n}_r \setminus \{n_r\}} \pm 1 \cdot \mp 1 \cdot \mu(n_r/d) \, d \\
&= - \sum_{d \in \underline{n}_r \setminus \{n_r\}} \mu(n_r/d) \, d \\
&= \mu(n_r/n_r) \, n_r - \sum_{d \in \underline{n}_r} \mu(n_r/d) \, d \\
&= n_r - \sum_{d|n_r} \mu(n_r/d) \, d \\
&= n_r - \varphi(n_r) \quad \text{by Lemma 14} \\
&= \psi(n_r)
\end{aligned}$$

Thus

$$\varepsilon^\pm(n) \geq \max_{\substack{1 \leq r < k \\ \rho(k-r) = \mp 1}} (\min \{p_{r+1}, n_r\} - \psi(n_r)) = \max_{\substack{1 \leq r < k \\ \rho(k-r) = \mp 1}} (\min \{p_{r+1}, p_1 \cdots p_r\} - \psi(p_1 \cdots p_r)) = \beta^\pm(n)$$

Hence

$$\begin{aligned}
g(\Phi_n) &\geq \varepsilon^+(n) \geq \beta^+(n) \\
g(\Psi_n) &\geq \varepsilon^-(n) \geq \beta^-(n)
\end{aligned}$$

The theorem has been proved. □

Proof of Theorem 3. We set $j = k$. Note

$$\varepsilon^\pm(n) \geq \max_{\substack{1 \leq r < k \\ \rho(k-r) = \mp 1}} \left(\min \{p_{k+1}, n_r\} - \sum_{\substack{d \in \underline{n} \\ \omega(d) < r}} \pm \mu(n/d) \, d \right) \quad \text{by Lemma 13}$$

Note

$$\min \{p_{k+1}, n_r\} = \min \{\infty, n_r\} = n_r$$

Thus

$$\varepsilon^\pm(n) \geq \max_{\substack{1 \leq r < k \\ \rho(k-r) = \mp 1}} \left(n_r - \sum_{\substack{d \in \underline{n} \\ \omega(d) < r}} \pm \mu(n/d) \, d \right) = \max_{\substack{1 \leq r < k \\ \rho(k-r) = \mp 1}} \left(p_1 \cdots p_r - \sum_{\substack{d|n \\ \omega(d) < r}} \pm \mu(n/d) \, d \right) = \gamma^\pm(n)$$

Hence

$$\begin{aligned}
g(\Phi_n) &\geq \varepsilon^+(n) \geq \gamma^+(n) \\
g(\Psi_n) &\geq \varepsilon^-(n) \geq \gamma^-(n)
\end{aligned}$$

The theorem has been proved. □

5.3 Proof of Special bound δ^- (Theorem 4)

It is possible to prove Theorem 4 in a similar way to the last three theorems, by restricting B as mentioned in Section 2, that is,

$$B = \{d : d|p_1 \cdots p_k \text{ and } \omega(d) < k \text{ and } d \neq p_2 \cdots p_k\}.$$

However, it is simpler to prove it in a different way.

Lemma 15. *We have*

$$\Psi_n(x) = H(x) \left(x^{\frac{n}{p_1}} - 1 \right)$$

where $H(x) = \Phi_{n_{k-1}} \left(x^{\frac{n}{n_k}} \right) \Phi_{n_{k-2}} \left(x^{\frac{n}{n_{k-1}}} \right) \cdots \Phi_{n_1} \left(x^{\frac{n}{n_2}} \right)$.

Proof. Recall the well known property of cyclotomic polynomials

$$\Phi_{np}(x) = \frac{\Phi_n(x^p)}{\Phi_n(x)}$$

where p is a prime and not a factor of n . In terms of the inverse cyclotomic polynomial, it can be immediately restated as

$$\Psi_{np}(x) = \Phi_n(x) \Psi_n(x^p)$$

Repeatedly applying the above equality on $\Psi_n(x)$, we have

$$\begin{aligned} \Psi_n(x) &= \Phi_{n_{k-1}} \left(x^{\frac{n}{n_k}} \right) \Psi_{n_{k-1}} \left(x^{\frac{n}{n_{k-1}}} \right) \\ &= \Phi_{n_{k-1}} \left(x^{\frac{n}{n_k}} \right) \Phi_{n_{k-2}} \left(x^{\frac{n}{n_{k-1}}} \right) \Psi_{n_{k-2}} \left(x^{\frac{n}{n_{k-2}}} \right) \\ &= \cdots \\ &= \Phi_{n_{k-1}} \left(x^{\frac{n}{n_k}} \right) \Phi_{n_{k-2}} \left(x^{\frac{n}{n_{k-1}}} \right) \cdots \Phi_{n_1} \left(x^{\frac{n}{n_2}} \right) \Psi_{n_1} \left(x^{\frac{n}{p_1}} \right) \\ &= H(x) \Psi_{n_1} \left(x^{\frac{n}{p_1}} \right) \end{aligned}$$

Recall that for a prime p , we have

$$\Psi_p(x) = x - 1$$

Hence

$$\Psi_n(x) = H(x) \left(x^{\frac{n}{p_1}} - 1 \right)$$

□

Proof of Theorem 4. From Lemma 15 we have

$$\begin{aligned} \Psi_n(x) &= H(x) \left(x^{\frac{n}{p_1}} - 1 \right) \\ &= -H(x) + H(x) \cdot x^{\frac{n}{p_1}} \end{aligned}$$

Note

$$\begin{aligned} \deg(H(x)) &= \psi(n) - \frac{n}{p_1} \\ \text{tdeg} \left(H(x) \cdot x^{\frac{n}{p_1}} \right) &= \frac{n}{p_1} \end{aligned}$$

We have

$$\frac{n}{p_1} - \left(\psi(n) - \frac{n}{p_1} \right) = 2 \frac{n}{p_1} - \psi(n) = \delta^-(n)$$

If $\delta^-(n) \leq 0$, then there is nothing to show. If $\delta^-(n) > 0$ then there is a gap in $\Psi_n(x)$ between $x^{\psi(n) - \frac{n}{p_1}}$ and $x^{\frac{n}{p_1}}$. Therefore

$$g(\Psi_n) \geq \delta^-(n)$$

The theorem has been proved. □

5.4 Proof of Sufficient condition on $g(\Psi_n)$ (Theorem 6)

There are two claims in Theorem 6. We will prove them one by one.

Proof of Theorem 6 Claim 1. We will prove that $g(\Psi_n) = \delta^-(n)$ if $\delta^-(n) \geq \frac{1}{2} \frac{n}{p_1}$. From Lemma 15 we have

$$\Psi_n(x) = -H(x) + H(x) \cdot x^{\frac{n}{p_1}}$$

Let

$$\delta^-(n) = \text{tdeg} \left(H(x) \cdot x^{\frac{n}{p_1}} \right) - \deg(H(x))$$

Note that if $\delta^-(n) \geq \deg(H(x))$, then we obviously have $g(\Psi_n) = \delta^-(n)$. In the following we simplify the expression $\delta^-(n)$ and the condition $\delta^-(n) \geq \deg(H(x))$. First, we simplify the expression $\delta^-(n)$.

$$\begin{aligned} \delta^-(n) &= \text{tdeg} \left(H(x) \cdot x^{\frac{n}{p_1}} \right) - \deg(H(x)) \\ &= \frac{n}{p_1} - \left(\psi(n) - \frac{n}{p_1} \right) \\ &= 2 \frac{n}{p_1} - \psi(n) \end{aligned}$$

Next, we simplify the condition $\delta^-(n) \geq \deg(H(x))$.

$$\begin{aligned} \delta^-(n) \geq \deg(H(x)) &\iff 2 \frac{n}{p_1} - \psi(n) \geq \psi(n) - \frac{n}{p_1} \\ &\iff 3 \frac{n}{p_1} - 2 \psi(n) \geq 0 \\ &\iff \frac{3}{2} \frac{n}{p_1} - \psi(n) \geq 0 \\ &\iff 2 \frac{n}{p_1} - \psi(n) \geq \frac{1}{2} \frac{n}{p_1} \\ &\iff \delta^-(n) \geq \frac{1}{2} \frac{n}{p_1} \end{aligned}$$

Therefore we have shown if $\delta^-(n) \geq \frac{1}{2} \frac{n}{p_1}$ then $g(\Psi_n) = \delta^-(n)$ which proves the first claim of the theorem. \square

Before we prove the second claim of Theorem 6, we need a technical lemma.

Lemma 16. *If $p_2 > (k-1)(2p_1-3)$ then $\delta^-(n) \geq \frac{1}{2} \frac{n}{p_1}$.*

Proof. Note

$$\begin{aligned} \delta^-(n) &\geq \frac{1}{2} \frac{n}{p_1} \\ &\iff \frac{3}{2} \frac{n}{p_1} \geq \psi(n) \\ &\iff \frac{3}{2} \frac{n}{p_1} \geq n - \varphi(n) \\ &\iff \frac{3}{2} \frac{1}{p_1} \geq 1 - \frac{\varphi(n)}{n} \\ &\iff \frac{3}{2} \frac{1}{p_1} \geq 1 - \left(1 - \frac{1}{p_1} \right) \cdots \left(1 - \frac{1}{p_k} \right) \\ &\iff \frac{1}{2} \frac{1}{p_1} \geq 1 - \frac{1}{p_1} - \left(1 - \frac{1}{p_1} \right) \cdots \left(1 - \frac{1}{p_k} \right) \end{aligned}$$

$$\begin{aligned}
&\Leftrightarrow \frac{1}{2} \frac{1}{p_1} \geq \left(1 - \frac{1}{p_1}\right) \left(1 - \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)\right) \\
&\Leftrightarrow \frac{1}{2} \geq (p_1 - 1) \cdot \left(1 - \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)\right) \\
&\Leftrightarrow \frac{1}{2} \geq (p_1 - 1) \cdot \left(1 - \left(1 - \frac{1}{p_2}\right) \left(1 - \frac{1}{p_2 + 1}\right) \cdots \left(1 - \frac{1}{p_2 + k - 2}\right)\right) \\
&\Leftrightarrow \frac{1}{2} \geq (p_1 - 1) \cdot \left(1 - \left(\frac{p_2 - 1}{p_2}\right) \left(\frac{p_2}{p_2 + 1}\right) \left(\frac{p_2 + 1}{p_2 + 2}\right) \cdots \left(\frac{p_2 + k - 3}{p_2 + k - 2}\right)\right) \\
&\Leftrightarrow \frac{1}{2} \geq (p_1 - 1) \cdot \left(1 - \frac{p_2 - 1}{p_2 + k - 2}\right) \\
&\Leftrightarrow \frac{1}{2} \geq (p_1 - 1) \cdot \frac{k - 1}{p_2 + k - 2} \\
&\Leftrightarrow \frac{p_2 + k - 2}{2} \geq (k - 1)(p_1 - 1) \\
&\Leftrightarrow p_2 + k - 2 \geq (k - 1)(2p_1 - 2) \\
&\Leftrightarrow p_2 \geq (k - 1)(2p_1 - 2) - (k - 2) \\
&\Leftrightarrow p_2 \geq (k - 1)(2p_1 - 3) + 1 \\
&\Leftrightarrow p_2 > (k - 1)(2p_1 - 3).
\end{aligned}$$

Therefore, if $p_2 > (k - 1)(2p_1 - 3)$, then $\delta^-(n) \geq \frac{1}{2} \frac{n}{p_1}$. □

Proof of Theorem 6 Claim 2. We will prove

$$\lim_{b \rightarrow \infty} \frac{\#\left\{n : p_k \leq b, p_1 = p, \delta^-(n) \geq \frac{1}{2} \frac{n}{p_1}\right\}}{\#\{n : p_k \leq b, p_1 = p\}} = 1$$

Let q_i be the i -th odd prime, that is, $q_1 = 3, q_2 = 5, q_3 = 7, q_4 = 11$, etc. Let $k \geq 2$. Let $p = q_v$ and $b = q_w$. Then we have

$$\begin{aligned}
&\#\{n : p_k \leq b, p_1 = p\} \\
&= \#\{(p_1, \dots, p_k) : p_1 < \cdots < p_k \leq b, p_1 = p\} \\
&= \#\{(q_{i_1}, \dots, q_{i_k}) : q_{i_1} < \cdots < q_{i_k} \leq q_w, q_{i_1} = q_v\} \\
&= \#\{(i_1, i_2, \dots, i_k) : i_1 < i_2 < \cdots < i_k \leq w, i_1 = v\} \\
&= \#\{(i_2, \dots, i_k) : v + 1 \leq i_2 < \cdots < i_k \leq w\} \\
&= \#\{(i_2, \dots, i_k) : v + 1 \leq i_2 < \cdots < i_k \leq v + (w - v)\} \\
&= \binom{w - v}{k - 1}
\end{aligned}$$

Thus

$$\#\{n : p_k \leq b, p_1 = p\} = \binom{w - v}{k - 1}$$

Note

$$\begin{aligned}
&\#\left\{n : p_k \leq b, p_1 = p, \delta^-(n) \geq \frac{1}{2} \frac{n}{p_1}\right\} \\
&= \#\left\{(p_1, \dots, p_k) : p_k \leq b, p_1 = p, \delta^-(p_1 \cdots p_k) \geq \frac{1}{2} \frac{p_1 \cdots p_k}{p_1}\right\} \\
&\geq \#\{(p_1, \dots, p_k) : p_k \leq b, p_1 = p, p_2 > (k - 1)(2p_1 - 3)\} \quad (\text{from Lemma 16})
\end{aligned}$$

$$\begin{aligned}
&= \#\{(q_{i_1}, \dots, q_{i_k}) : q_{i_1} < \dots < q_{i_k} \leq q_w, q_{i_1} = q_v, q_{i_2} > (k-1)(2q_v-3)\} \\
&= \#\{(q_{i_1}, \dots, q_{i_k}) : q_{i_1} < \dots < q_{i_k} \leq q_w, q_{i_1} = q_v, q_{i_2} \geq q_y\} \text{ where } y = \underset{q_i > (k-1)(2q_v-3)}{\operatorname{argmin}} i \\
&= \#\{(i_1, \dots, i_k) : i_1 < \dots < i_k \leq w, i_1 = v, i_2 \geq y\} \\
&= \#\{(i_2, \dots, i_k) : v+1 \leq i_2 < \dots < i_k \leq w, i_2 \geq y\} \\
&= \#\{(i_2, \dots, i_k) : \max\{v+1, y\} \leq i_2 < \dots < i_k \leq w\} \\
&= \#\{(i_2, \dots, i_k) : y \leq i_2 < \dots < i_k \leq w\} \quad (\text{since } y \geq v+1) \\
&= \binom{w-y+1}{k-1}
\end{aligned}$$

Thus we have

$$\#\left\{n : p_k \leq b, p_1 = p, \delta^-(n) \geq \frac{1}{2} \frac{n}{p_1}\right\} \geq \binom{w-y+1}{k-1}$$

Note

$$\lim_{b \rightarrow \infty} \frac{\#\left\{n : p_k \leq b, p_1 = p, \delta^-(n) \geq \frac{1}{2} \frac{n}{p_1}\right\}}{\#\{n : p_k \leq b, p_1 = p\}} \geq \lim_{w \rightarrow \infty} \frac{\binom{w-y+1}{k-1}}{\binom{w-v}{k-1}} = \lim_{w \rightarrow \infty} \frac{\frac{1}{(k-1)!} w^{k-1} + \dots}{\frac{1}{(k-1)!} w^{k-1} + \dots} = 1$$

Since

$$\lim_{b \rightarrow \infty} \frac{\#\left\{n : p_k \leq b, p_1 = p, \delta^-(n) \geq \frac{1}{2} \frac{n}{p_1}\right\}}{\#\{n : p_k \leq b, p_1 = p\}} \leq 1$$

we can conclude

$$\lim_{b \rightarrow \infty} \frac{\#\left\{n : p_k \leq b, p_1 = p, \delta^-(n) \geq \frac{1}{2} \frac{n}{p_1}\right\}}{\#\{n : p_k \leq b, p_1 = p\}} = 1$$

which proves the second claim of the theorem. \square

6 Evidence for Equivalent condition on $g(\Phi_n)$ (Conjecture 7)

Let us recall the conjecture: $g(\Phi_n) = \varphi(p_1 \cdots p_{k-1})$ if and only if $p_k > p_1 \cdots p_{k-1}$. The conjecture is trivially true for $k = 1$. In [17], the conjecture is proved for $k = 2$. For $k \geq 3$ the conjecture is still open. One way to check (support or disprove) the conjecture is to compute Φ_n for many n with $k \geq 3$ and to check whether the maximum gap is $\varphi(p_1 \cdots p_{k-1})$ or not. We did this for n up to 40,000, without finding any counter-example. However, this method only shows that the conjecture is true for finitely many such n .

In this section, we will describe an algorithm (Algorithm 1) which allows the conjecture to be checked for infinitely many such n and we will report that we have done so (Theorem 18). For the sake of notational simplicity, let $m = p_1 \cdots p_{k-1}$ and $p = p_k$. Then the above conjecture can be restated as: $g(\Phi_{mp}) = \varphi(m)$ if and only if $p > m$. The algorithm (which will be given later) is based on the following theorem.

Theorem 17 (Invariance). *Let m be odd square-free. Let $p, p' > m$ be primes such that $p \equiv_m p'$. Then*

$$g(\Phi_{mp}) = g(\Phi_{mp'})$$

Proof. Let m be odd square-free. Let $p > m$ be prime. We will divide the proof into several steps.

1. Let $q = \operatorname{quo}(p, m)$ and $r = \operatorname{rem}(p, m)$. Let

$$\Phi_{mp} = \sum_{i=0}^{\varphi(m)-1} f_{m,p,i} x^{ip} \quad \deg f_{m,p,i} < p$$

$$f_{m,p,i} = \sum_{j=0}^q f_{m,p,i,j} x^{jm} \quad \deg f_{m,p,i,j} < m$$

We recall the following results from [1]: For all $0 \leq i \leq \varphi(m) - 1$, we have

- (C1) $f_{m,p,i,0} = \dots = f_{m,p,i,q-1}$
- (C2) $f_{m,p,i,q} = \text{rem}(f_{m,p,i,0}, x^r)$
- (C3) $f_{m,p,i,0} = f_{m,p',i,0}$ if $p \equiv_m p'$

2. From $\Phi_{mp} = \sum_{i=0}^{\varphi(m)-1} f_{m,p,i} x^{ip}$, we have

$$g(\Phi_{mp}) = \max \left\{ \max_{0 \leq i \leq \varphi(m)-1} g(f_{m,p,i}), \max_{0 \leq i \leq \varphi(m)-2} (p + \text{tdeg}(f_{m,p,i+1}) - \text{deg}(f_{m,p,i})) \right\} \quad (1)$$

3. From $f_{m,p,i} = \sum_{j=0}^q f_{m,p,i,j} x^{jp}$ and (C1) and (C2), we have

$$\begin{aligned} g(f_{m,p,i}) &= \max \{g(f_{m,p,i,0}), g(f_{m,p,i,q}), m + \text{tdeg}(f_{m,p,i,0}) - \text{deg}(f_{m,p,i,0})\} \\ &= \max \{g(f_{m,p,i,0}), m + \text{tdeg}(f_{m,p,i,0}) - \text{deg}(f_{m,p,i,0})\} \end{aligned} \quad (2)$$

4. From $p - qm = r$, we have

$$\begin{aligned} p + \text{tdeg}(f_{m,p,i+1}) - \text{deg}(f_{m,p,i}) &= \begin{cases} p + \text{tdeg}(f_{m,p,i+1,0}) - ((q-1)m + \text{deg}(f_{m,p,i,0})) & \text{if } f_{m,p,i,q} = 0 \\ p + \text{tdeg}(f_{m,p,i+1,0}) - (qm + \text{deg}(f_{m,p,i,q})) & \text{else} \end{cases} \\ &= \begin{cases} r + m + \text{tdeg}(f_{m,p,i+1,0}) - \text{deg}(f_{m,p,i,0}) & \text{if } f_{m,p,i,q} = 0 \\ r + \text{tdeg}(f_{m,p,i+1,0}) - \text{deg}(\text{rem}(f_{m,p,i,0}, x^r)) & \text{else} \end{cases} \end{aligned} \quad (3)$$

5. Combining the equalities (1), (2) and (3), we see $g(\Phi_{mp})$ depends *only on* m, r and $f_{m,p,i,0}$.

6. Let $p' > m$ be a prime other than p . Then $g(\Phi_{mp'})$ also depends *only on* m, r' and $f_{m,p',i,0}$.

7. Suppose $p \equiv_m p'$. Then obviously $r = r'$. Furthermore from (C3), we have $f_{m,p,i,0} = f_{m,p',i,0}$. Thus $g(\Phi_{mp}) = g(\Phi_{mp'})$.

□

From the above theorem (Theorem 17) we immediately obtain the following algorithm.

Algorithm 1 (Checking the conjecture).

In: m , odd square-free, say $m = p_1 \cdots p_{k-1}$ and $p_1 < \cdots < p_k$

Out: truth of the claim that $\forall_{\text{prime } p > p_{k-1}} [g(\Phi_{mp}) = \varphi(m) \iff p > m]$

1. for p from $p_{k-1} + 1$ to $m - 1$, p prime, do

- (a) $F \leftarrow \Phi_{mp}$
- (b) $g \leftarrow$ the maximum gap of F
- (c) if $g = \varphi(m)$ then return false

2. for r from 1 to $m - 1$, where $\gcd(m, r) = 1$, do

- (a) $p \leftarrow$ the smallest prime larger than m such that $\text{rem}(m, p) = r$

- (b) $F \leftarrow \Phi_{mp}$
- (c) $g \leftarrow$ the maximum gap of F
- (d) if $g \neq \varphi(m)$ then return false

3. return true

We have implemented the above algorithm in C language. The cyclotomic polynomials were computed using the algorithm called Sparse Power Series (Algorithm 4 in [2]) because it is the fastest known algorithm for inputs where p is not very big compared to m . The code for the algorithm has been kindly provided by Andrew Arnold, one of the authors of [2]. By executing the program, so far we have proved the following.

Theorem 18 (Evidence of the conjecture for infinitely many primes). *For all primes p and $m < 1000$, we have*

$$g(\Phi_{mp}) = \varphi(m) \text{ if and only if } p > m$$

In other words, for all k and for all p_1, \dots, p_k such that $p_1 \cdots p_{k-1} < 1000$, we have

$$g(\Phi_{p_1 \cdots p_k}) = \varphi(p_1 \cdots p_{k-1}) \text{ if and only if } p_k > p_1 \cdots p_{k-1}.$$

The above computation took 86 minutes on a MacBook Pro (CPU: 2.4 GHz Intel Core i5, Memory: 16 GB 1600 MHz DDR3). Of course, one could continue to check larger m values using larger computing resources.

References

- [1] AL-KATEEB, A., HONG, H., AND LEE, E. Structure of cyclotomic polynomials and several applications. *ArXiv* (2017).
- [2] ARNOLD, A., AND MONAGAN, M. Calculating cyclotomic polynomials. *Mathematics of Computation* (2011).
- [3] BACHMAN, G. On the coefficients of ternary cyclotomic polynomials. *J. of Number Theory* 100 (2003), 104–116.
- [4] BEITER, M. Coefficients of the cyclomic polynomial $f_{3qr}(x)$. *Fibonacci Quart.* 16 (1978), 302–306.
- [5] BZDEGA, B. Bounds on ternary cyclotomic coefficients. *Acta Arith.* 144 (2010), 5–16.
- [6] BZDEGA, B. On the height of cyclotomic polynomials. *Acta Arith.* 152 (2012), 349–359.
- [7] BZDEGA, B. Jumps of ternary cyclotomic coefficients. *Acta Arith.* 163 (2014), 203–213.
- [8] BZDEGA, B. On a certain family of inverse ternary cyclotomic polynomials. *J. Number Theory* 141 (2014), 1–12.
- [9] CAMBURU, O.-M., CIOLAN, E.-A., LUCA, F., MOREE, P., AND SHPARLINSKI, I. E. Cyclotomic coefficients: gaps and jumps. *J. Number Theory* 163 (2016), 211–237.
- [10] COBELI, C., GALLOT, Y., MOREE, P., AND ZAHARESCU, A. Sister beiter and kloosterman: a tale of cyclotomic coefficients and modular inverses. *Indag. Math. (N.S.)* 24 (2013), 915–929.
- [11] DRESDEN, G. P. On the middle coefficient of a cyclotomic polynomial. *Amer. Math. Monthly* 111 (2004), 531–533.
- [12] FINTZEN, J. Cyclotomic polynomial coefficients $a(n, k)$ with n and k in prescribed residue classes. *J. Number Theory* 131 (2011), 1852–1863.

- [13] FOUVRY, E. On binary cyclotomic polynomials. *Algebra Number Theory* 5 (2013), 1207–1223.
- [14] GALLOT, Y., AND MOREE, P. Neighboring ternary cyclotomic coefficients differ by at most one. *J. Ramanujan Math. Soc.* 24 (2009), 235–248.
- [15] GALLOT, Y., AND MOREE, P. Ternary cyclotomic polynomials having a large coefficient. *J. Reine Angew. Math.* 632 (2009), 105–125.
- [16] GALLOT, Y., MOREE, P., AND WILMS, R. The family of ternary cyclotomic polynomials with one free prime. *Involve* 4 (2011), 317–341.
- [17] HONG, H., LEE, E., LEE, H.-S., AND PARK, C.-M. Maximum gap in (inverse) cyclotomic polynomial. *J. of Number Theory* (2012).
- [18] HONG, H., LEE, E., LEE, H.-S., AND PARK, C.-M. Simple and exact formula for minimum loop length in ate_i pairing based on brezing-weng curves. *Des. Codes Cryptogr.* 67 (2013), 271–292.
- [19] KAPLAN, N. Flat cyclotomic polynomials of order three. *J. Number Theory* 127 (2007), 118–126.
- [20] LEE, E., LEE, H.-S., AND PARK, C.-M. Efficient and generalized pairing computation on abelian varieties. *IEEE Trans. Inform. Theory* 55 (2009), 1793–1803.
- [21] LEHMER, E. On the magnitude of the coefficients of the cyclotomic polynomials. *Bull. Amer. Math. Soc* 42 (1936), 389–392.
- [22] MOREE, P. Inverse cyclotomic polynomials. *J. of Number Theory* (2009).
- [23] MOREE, P. Numerical semigroups, cyclotomic polynomials and bernoulli numbers. *arXiv* (2013).
- [24] MOREE, P., AND ROSU, E. Non-beiter ternary cyclotomic polynomials with an optimally large set of coefficients. *Int. J. Number Theory* 8 (2012), 1883–1902.
- [25] THANGADURAI, R. On the coefficients of cyclotomic polynomials. *Cyclotomic Fields and Related Topics, Pune* (2000), 311–322.
- [26] ZHANG, B. Remarks on the maximum gap in binary cyclotomic polynomials. *Bull. Math. Soc. Sci. Math. Roumanie* (2015).
- [27] ZHAO, C.-A., ZHANG, F., AND HUANG, J. A note on the ate pairing. *Int. J. Inf. Secur.* 7 (2008), 379–382.